

# METHOD AND SYSTEM FOR PERMITTING USE OF IC CARD SERVICE TO MULTIPLE SERVICE USER

Patent number: JP2004102784  
Publication date: 2004-04-02  
Inventor: HASHIMOTO JUNKO; KASHIWAGI TAKUMI; NIWANO EIICHI; MINAMI HIROYUKI  
Applicant: NIPPON TELEGRAPH & TELEPHONE  
Classification:  
- International: G06F15/00; G06K17/00; G09C1/00; H04L9/32; G06F15/00; G06K17/00; G09C1/00; H04L9/32; (IPC1-7): G06F15/00; G06F17/60; G06K17/00; G09C1/00; H04L9/32  
- european:  
Application number: JP20020265385 20020911  
Priority number(s): JP20020265385 20020911

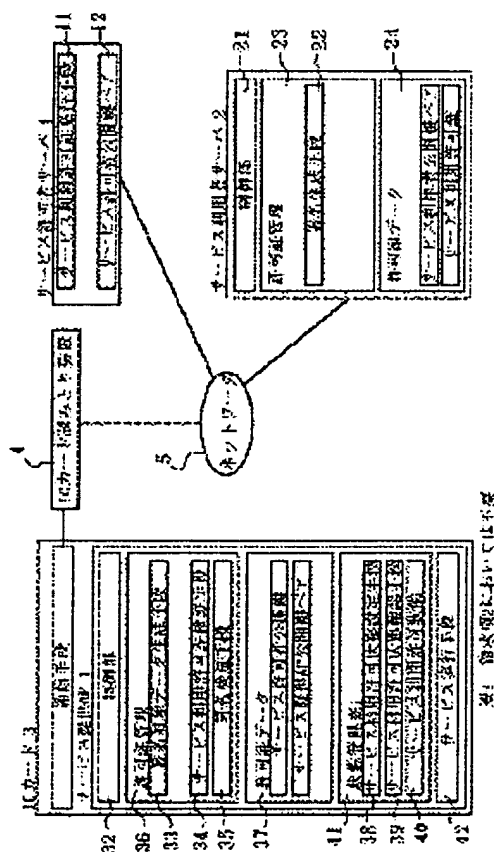
Report a data error here

## Abstract of JP2004102784

**PROBLEM TO BE SOLVED:** To provide a method and a system for permitting use of IC card service allowing a service providing application in an IC card to be used by multiple enterprises.

**SOLUTION:** This system comprises a service permitting person's server, one or more service user servers, and IC cards used by inserting an IC card reader having a means for communicating with the service user servers. The service permitting person's server issues a use permission certificate for the service providing application stored in the IC card to one or more service user servers. The service providing application stored in the IC card verifies the service use permission certificate sent from the service user servers and, after the authentication, performs the service only when the type of the service requested by a service execution request from the service user servers matches the type of the service included in the service use certificate.

COPYRIGHT: (C)2004,JPO



Data supplied from the [esp@cenet](mailto:esp@cenet) database - Worldwide

BEST AVAILABLE COPY

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-102784

(P2004-102784A)

(43) 公開日 平成16年4月2日(2004.4.2)

(51) Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
G06F 15/00	G06F 15/00 330G	5B058
G06F 17/60	G06F 17/60 126A	5B085
G06K 17/00	G06K 17/00 L	5J104
G09C 1/00	G09C 1/00 640D	
H04L 9/32	H04L 9/00 675B	

審査請求 未請求 請求項の数 12 O L (全 19 頁) 最終頁に続く

(21) 出願番号	特願2002-265385 (P2002-265385)	(71) 出願人	000004226
(22) 出願日	平成14年9月11日 (2002.9.11)		日本電信電話株式会社
			東京都千代田区大手町二丁目3番1号
特許法第30条第1項適用申請有り 2002年3月15日 社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告 信学技報 Vol. 101 No. 742」に発表		(74) 代理人	100072051
			弁理士 杉村 興作
		(72) 発明者	橋本 順子
			東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
		(72) 発明者	柏木 巧
			東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
		(72) 発明者	庭野 栄一
			東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

最終頁に続く

(54) 【発明の名称】 複数サービス利用者に対するICカードサービス利用許可方法及びシステム

## (57) 【要約】

【課題】 ICカード内のサービス提供アプリケーションを複数の事業者に対して利用可能とするICカードサービス利用許可方法及びシステムを提供することにある。

【解決手段】 サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったICカード読取装置に挿入されて利用されるICカードを備えたシステムにおいて、 サービス許可者サーバが、一つ以上のサービス利用者サーバに対し、 ICカードに格納されたサービス提供アプリケーションの利用許可証を発行し、 ICカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから送られてくるサービス利用許可証を検証し、認証後に、サービス利用者サーバからのサービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う。

【選択図】 図4

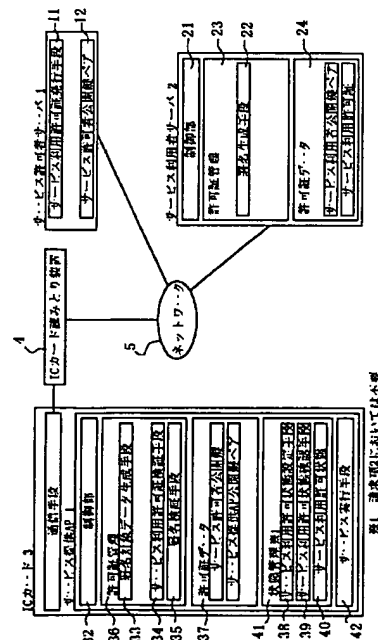


図1 請求項1においては本要

## 【特許請求の範囲】

## 【請求項 1】

サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持った IC カード読取装置に挿入されて利用される IC カードからなるシステムにおいて、

サービス許可者サーバが、一つ以上のサービス利用者サーバに対し、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報 (AID) と、サービスの種類 (オペレーションの種類) を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス利用許可証を発行し、

10

サービス利用許可証を持つサービス利用者サーバは、IC カード内に格納されたサービス提供アプリケーションを利用する際に、IC カードに格納されたサービス提供アプリケーションから受け取ったチャレンジなどの署名対象データをサービス利用者秘密鍵で暗号化して署名を作成し、その署名データとサービス利用許可証を IC カードに格納されたサービス提供アプリケーションに送信し、

IC カードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、

これらの検証が成功したとき、サービス利用許可証に含まれるサービス利用許可情報を記録するとともに、サービス利用許可証の検証の成功をサービス利用者サーバに返し、

20

サービス利用者サーバから、サービス利用許可証に対応するサービスの実行要求を受信したとき、保持したサービス利用許可情報を確認し、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする、

IC カードサービス利用許可方法。

## 【請求項 2】

請求項 1 に記載の方法において、

サービス利用者サーバは、IC カードに格納されたサービス提供アプリケーションから署名対象データを受け取った後に、この署名対象データとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともに IC カードに送り、

30

IC カードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、

これらの検証が成功したとき、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする、

IC カードサービス利用許可方法。

40

## 【請求項 3】

請求項 1 又は 2 に記載の方法において、

サービス許可者サーバは、IC カードに格納されたサービス提供アプリケーションに、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス提供許可証を発行し、

サービス利用者サーバは、チャレンジなどの署名対象データを IC カードに送り、

IC カード内のサービス提供アプリケーションは、受信した署名対象データに対しサービス提供アプリケーションの秘密鍵で署名を行い、その署名データと、サービス提供許可証をサービス利用者サーバに送り、

50

サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、保持しているサービス許可者公開鍵を用いてサービス提供許可証を検証するとともに、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証することを特徴とする、

ＩＣカードサービス利用許可方法。

【請求項４】

請求項１～３の何れかに記載の方法において、

サービス利用許可証のデータに、当該サービス提供アプリケーションが管理するデータの種類の種類が含まれ、

サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみであることを特徴とする、

ＩＣカード利用許可方法。

【請求項５】

請求項１～４の何れかに記載の方法において、

サービス許可者サーバが、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する、ことを特徴とするＩＣカードサービス利用許可方法。

【請求項６】

サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったＩＣカード読取装置に挿入されて利用されるＩＣカードからなるシステムにおいて、

サービス許可者サーバが、一つ以上のサービス利用者サーバに対し、サービス利用許可証を発行するサービス利用許可証発行手段を持ち、

サービス利用許可証は、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報（ＡＩＤ）と、サービスの種類（オペレーションの種類）、を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、

ＩＣカードに格納されたサービス提供アプリケーションは、チャレンジなどを生成する署名対象データ生成手段を持ち、

サービス利用者サーバは、サービス利用許可証を保持しており、ＩＣカードに格納されたサービス提供アプリケーションから受け取った署名対象データにサービス利用者サーバの秘密鍵で署名を行う、署名生成手段を持ち、

ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データと、サービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証する、サービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する、署名検証手段と

、検証が成功した場合に、サービス利用許可証に含まれるサービス利用許可情報を保持するサービス利用許可状態設定手段を持ち、

サービス利用者サーバから、サービス実行要求が送信された場合に、保持したサービス利用許可情報を確認するサービス利用許可状態確認手段を持ち、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことを特徴とする、

ＩＣカードサービス利用許可システム。

【請求項７】

請求項６に記載のシステムにおいて、

ＩＣカードに格納されたサービス提供アプリケーションは、チャレンジなどを生成する署名対象データ生成手段を持ち、

10

20

30

40

50

サービス利用者サーバは、サービス利用許可証を保持しており、ＩＣカードに格納されたサービス提供アプリケーションへのサービス実行要求を含むデータもしくはそのダイジェスト情報に、サービス利用者サーバの秘密鍵で署名を行う、署名生成手段を持ち、

ＩＣカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データと、サービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証する、サービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する、署名検証手段と

、  
検証が成功した場合に、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことを特徴とする、

10

ＩＣカードサービス利用許可システム。

【請求項 8】

請求項 6 又は 7 に記載のＩＣカードサービス利用許可システムにおいて、

サービス許可者サーバが、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供許可証を発行するサービス提供許可証発行手段を持ち、

サービス提供許可証は、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、

サービス利用者サーバが、チャレンジなどを生成する署名対象データ生成手段を持ち、

20

サービス提供アプリケーションが、サービス利用者サーバから受け取った署名対象データに対し、サービス提供アプリケーションの秘密鍵で署名を行う、署名生成手段を持ち、

サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サ

サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データ

を検証する署名検証手段と、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段を持つことを特徴とする、

ＩＣカードサービス利用許可システム。

【請求項 9】

請求項 6 ～ 8 の何れかに記載のＩＣカードサービス利用許可システムにおいて、

30

サービス利用許可証の署名対象データに、当該サービス提供アプリケーションが管理するデータの種類が含まれ、

サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみであることを特徴とする、

ＩＣカード利用許可システム。

【請求項 10】

請求項 6 ～ 9 の何れかに記載のＩＣカードサービス利用許可システムにおいて、

サービス許可者サーバが、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する、課金情報登録手段を持つことを特徴とする、

40

ＩＣカードサービス利用許可システム。

【請求項 11】

請求項 1 ～ 5 の何れかに記載の方法を実行するためのコンピュータプログラム。

【請求項 12】

請求項 11 記載のコンピュータプログラムを記録したコンピュータ読取可能記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はＩＣカードサービス提供システムに関し、特に、ＩＣカード内のサービス提供ア

50

アプリケーションを複数の事業者が利用することを可能とするＩＣカードサービス利用許可方法及びシステムに関する。

【０００２】

【従来の技術】

従来のＩＣカードサービスシステムでは、サービス提供アプリケーションへのアクセス制御を行う主体と、サービス提供アプリケーションへの（アクセス制御の対象となる）アクセスを行う主体は、分離されていなかった。

そして、サービス提供アプリケーションが、適切なサービス利用者サーバに対してのみサービス提供を行うために、アクセス制御を行う場合、そのアクセス制御の基となる情報を、実際にアクセス制御の対象となるアクセスが行われる前に、サービス提供アプリケーションに予め設定していた。

以降、このアクセス制御の基となる情報を、暗号コードと呼ぶ。この暗号コードは、共通鍵・公開鍵である場合もある。この暗号コードと、暗号コードに対応するアクセス時の入力情報を、サービス提供アプリケーションに含まれる認証プロトコルに入力することによって、サービス提供アプリケーションは、正当なアクセス者を認証することができる。

従って、アクセス者は、暗号コードに対応する入力情報を作成する手段及び情報を保持しておく必要がある。この手段及び情報は、最も単純な場合には、サービス提供アプリケーションの持つ暗号コードと一致する暗号コードであり、認証プロトコルとして共通鍵認証を用いる場合には、サービス提供アプリケーションが持つ暗号コードである共通鍵で任意の情報を暗号化したものである。

従来のＩＣカードサービスシステムでは、ＩＣカード内のサービス提供アプリケーションに暗号コードを設定した主体が、同時に暗号コードに対応する入力情報を作成する手段及び情報を保持しており、サービス提供アプリケーションへのアクセスを行っていた。

【０００３】

【発明が解決しようとする課題】

しかし、これら暗号コードに対応する入力情報を作成する手段及び情報を、他の事業主体に安全に分配する手段については、発明されていなかった。

従って、従来のＩＣカードシステムでは、以下のような問題があった。

第一の問題点は、１つのサービス提供アプリケーションを複数の事業者で安全に共有することができないことである。

第二の問題点は、１つのサービス提供アプリケーションが保持する情報を複数の事業者で共有することができないことである。

第三の問題点は、１つのサービス提供アプリケーションを複数の事業者に共有した場合に、適切な課金の仕組みがないことである。ここで、サービス提供アプリケーションは、同一カード内の他のサービス提供アプリケーションによって利用されるライブラリのようなサービス提供アプリケーションも含むとする。

このため、あるサービス利用者がサービス提供アプリケーションの機能を利用する場合に、同一機能を持ったサービス提供アプリケーションが既にＩＣカード内に存在していても、自分専用のサービス提供アプリケーションを新たにＩＣカードに格納する必要があった。

従って、従来、利用者は、あるサービスの提供を複数の事業者から受ける場合に、その機能を持ったサービス提供アプリケーションを、複数、カード内に持つ必要があった。

【０００４】

本発明の目的は、これらの問題点を解決し、あるサービス提供アプリケーションを保持する業者が、他事業者に対し、安全にそのサービス利用権を貸与できる方法及びシステムを提供することにある。また、その際、貸与に対する課金の仕組みを提供することにある。これらの仕組みによって、複数の事業者がサービス提供アプリケーションを開発することなく、容易にサービスの提供を受けることが可能となる。また、１つのサービス提供アプリケーションを複数の事業者が共有することによって生まれる、付加価値サービスが可能となる。

## 【0005】

## 【課題を解決するための手段】

これらの問題を解決するために、請求項1に記載の発明は、

サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったICカード読取装置に挿入されて利用されるICカードからなるシステムにおいて、

サービス許可者サーバが、一つ以上のサービス利用者サーバに対し、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報(AID)と、サービスの種類(オペレーションの種類)を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス利用許可証を発行し、

10

サービス利用許可証を持つサービス利用者サーバは、ICカードに格納されたサービス提供アプリケーションを利用する際に、ICカードに格納されたサービス提供アプリケーションから受け取った署名対象データをサービス利用者公開鍵で暗号化して署名を作成し、その署名データとサービス利用許可証をICカードに格納されたサービス提供アプリケーションに送信し、

ICカードに格納されたサービス提供アプリケーションは、受信した署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、

20

これらの検証が成功したとき、サービス利用許可証に含まれるサービス利用許可情報を記録するとともに、サービス利用許可証の検証の成功をサービス利用者サーバに返送し、サービス利用者サーバから、サービス利用許可証に対応するサービスの実行要求を受信したとき、保持したサービス利用許可情報を確認し、サービス実行要求で要求されたサービスの種類がサービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする。

## 【0006】

また、請求項6に記載の発明は、この請求項1に記載の方法を実施するシステムであって、サービス許可者サーバと、一つ以上のサービス利用者サーバと、サービス利用者サーバと通信する手段を持ったICカード読取装置に挿入されて利用されるICカードからなるシステムにおいて、

30

サービス許可者サーバは、一つ以上のサービス利用者サーバに対し、サービス利用許可証を発行するサービス利用許可証発行手段を持ち、

サービス利用許可証は、発行先サービス利用者サーバの公開鍵と、サービス利用者に許可されたサービスを示すサービス提供アプリケーション識別情報(AID)と、サービスの種類(オペレーションの種類)、を含むサービス利用許可情報もしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、

ICカードに格納されたサービス提供アプリケーションは、チャレンジなどの署名対象データを生成する署名対象データ生成手段を持ち、

サービス利用者サーバは、サービス利用許可証を保持しており、ICカードに格納されたサービス提供アプリケーションから受け取った署名対象データにサービス利用者サーバの秘密鍵で署名を行う署名生成手段を持ち、

40

ICカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する署名検証手段と、

検証が成功した場合に、サービス利用許可証に含まれるサービス利用許可情報を保持するサービス利用許可状態設定手段を持ち、

サービス利用者サーバから、サービス実行要求が送信された場合に、サービス利用許可情報を確認するサービス利用許可状態確認手段を持ち、サービス実行要求で要求されたサー

50

ビスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行う、サービス実行手段を持つことをとする。

【0007】

請求項1及び6に記載の発明では、サービス利用許可証を持つ者のみが、サービス提供アプリケーションによって、サービス利用許可証で指定されたサービスの提供を受けることができる。また、サービス利用許可証は、複数の業者に対して、サービスの種類を指定して発行が可能である。

従って、サービス許可者は、サービス提供アプリケーションを利用してよいサービス利用者サーバと事前に契約を行ってサービス利用許可証を発行することで、複数のサービス利用者に対して、きめ細やかなサービスの利用許可を行うことができる。

10

さらに、サービス利用許可証を発行するためには、サービス許可者の秘密鍵で署名を行うことが必要であるため、サービス利用許可証の第三者による不正な発行を防ぐことが可能である。また、サービス利用許可証にはサービス利用者の公開鍵が含まれるため、サービス利用許可証の第三者による不正な利用を防ぐことが可能である。

従って、本発明は、上記技術により、あるサービス提供アプリケーションを実行する権限を持つサービス許可者が、そのサービス提供アプリケーションを実行する権限を、複数のサービス利用者に対して安全に委譲することを可能としている。

【0008】

請求項2に記載の発明は、請求項1に記載の方法において、

サービス利用者サーバは、ICカードに格納されたサービス提供アプリケーションから署名対象データを受け取った後に、この署名対象データとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともにICカードに送り、

20

サービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対して、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するとともに、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証し、

これらの検証が成功したとき、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うことを特徴とする。

30

【0009】

また、請求項7に記載の発明は、請求項2に記載の方法を実施するシステムであって、請求項6に記載のシステムにおいて、

サービス利用者サーバは、ICカードに格納されたサービス提供アプリケーションから受け取った署名対象データとサービス提供アプリケーションへのサービス実行要求を含むデータもしくはそのダイジェスト情報に、サービス利用者サーバの秘密鍵で署名を行う署名生成手段を持ち、

ICカードに格納されたサービス提供アプリケーションは、サービス利用者サーバから受け取った署名データとサービス利用許可証に対し、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段と、サービス利用許可証に含まれるサービス利用者公開鍵を用いて署名データを検証する署名検証手段と、

40

検証が成功した場合に、サービス実行要求で要求されたサービスの種類が、サービス利用許可証に含まれるサービスの種類と一致する場合にのみサービスの実行を行うサービス実行手段を持つことを特徴とする。

【0010】

請求項1及び6に記載の発明では、サービス提供アプリケーションからサービスの提供を受けるにあたって、事前にサービス利用許可証を提示し、認証を行っていたが、請求項2及び7に記載の発明では、事前の認証は行わず、サービス提供アプリケーションへのサービス要求時に、サービス利用許可証の確認を行うものである。

【0011】

50



請求項 3 記載の発明は、請求項 1 又は 2 記載の方法において、

サービス許可者サーバは、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションにおける識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであるサービス提供許可証を発行し、

サービス利用者サーバは、チャレンジなどの署名対象データをＩＣカードに送り、

ＩＣカード内のサービス提供アプリケーションは、受信した署名対象データに対しサービス提供アプリケーションの秘密鍵で署名を行い、その署名データと、サービス提供許可証をサービス利用者サーバに送り、

サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、保持しているサービス許可者公開鍵を用いてサービス提供許可証を検証するとともに、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証する、  
ことを特徴とする。

【 0 0 1 2 】

また、請求項 8 に記載の発明は、請求項 3 に記載の方法を実施するシステムであって、請求項 6 又は 7 記載のシステムにおいて、

サービス許可者サーバは、ＩＣカードに格納されたサービス提供アプリケーションに、サービス提供許可証を発行するサービス提供許可証発行手段を持ち、

サービス提供許可証は、サービス提供アプリケーションの公開鍵と、サービス提供アプリケーションの識別子を含むデータもしくはそのダイジェスト情報に対し、サービス許可者サーバの秘密鍵で署名を行ったデータであり、

サービス利用者サーバは、チャレンジなどの署名対象データを生成する署名対象データ生成手段を持ち、

サービス提供アプリケーションは、サービス利用者サーバから受け取った署名対象データに対し、サービス提供アプリケーションの秘密鍵で署名を行う、署名生成手段を持ち、

サービス利用者サーバは、サービス提供アプリケーションの正当性を確認するために、サービス提供アプリケーションから受け取った署名データと、サービス提供許可証に対し、サービス提供許可証に含まれるサービス提供アプリケーション公開鍵を用いて署名データを検証する署名検証手段と、保持しているサービス許可者公開鍵を用いてサービス利用許可証を検証するサービス利用許可証検証手段を持つことを特徴とする。

【 0 0 1 3 】

請求項 1 ～ 2 及び 6 ～ 7 に記載の発明では、サービス提供アプリケーションが、適切なサービス利用者を確認するための手段を提供していたが、請求項 3 及び 8 に記載の発明では、サービス利用者サーバが、通信相手である、サービス提供アプリケーションを確認する手段を提供している。

従って、請求項 3 及び 8 に記載の発明は、あるサービス提供アプリケーションを実行する権限を持つサービス許可者から、そのサービス提供アプリケーションを実行する権限を委譲された複数のサービス利用者が、不正なサービス提供アプリケーションからサービスの提供を受けることなく、安全にサービス利用することを可能としている。

従って、本発明によれば、あるサービス提供アプリケーションが提供するサービスを複数のサービス提供者間で安全に共有することが可能となる。

【 0 0 1 4 】

請求項 4 又は 9 に記載の発明は、請求項 1 ～ 3 又は 6 ～ 8 の何れかに記載の方法又はシステムにおいて、

サービス利用許可証の署名対象データに、当該サービス提供アプリケーションが管理するデータの種類が含まれ、

サービス提供の対象となるのは、サービス利用許可証で指定されたサービスの種類（オペレーション）で、サービス利用許可証で指定された種類のデータにアクセスする場合のみ

10

20

30

40

50

である、  
ことを特徴とする。

【0015】

請求項1～8又は6～8に記載の発明では、サービス利用許可の対象が、サービス提供アプリケーションの提供するサービスの種類（オペレーションの種類）であったが、請求項4、9に記載の本発明にあっては、サービス利用許可の対象として、そのサービス（オペレーション）が対象とするデータの種類の種類まで限定することによって、細やかなサービス利用許可を実現するものである。

従って、本発明によれば、あるサービス提供アプリケーションが保持するデータを複数のサービス利用許可者間で安全に共有することが可能となる。

10

【0016】

請求項5又は10に記載の本発明は、請求項1～4又は6～9の何れかに記載の方法又はシステムにおいて、

サービス許可者サーバは、サービス利用者サーバへのサービス利用許可証を発行した際に、サービス許可者サーバ内へ、発行履歴を課金情報として登録する課金情報登録手段を持つことを特徴とする。

請求項5及び10に記載の発明では、請求項1～4又は6～9に記載の方法及びシステムで発行されたサービス利用許可証を、課金情報として利用する手段を提供している。

【0017】

【発明の実施の形態】

20

次に、本発明の実施の形態について図面を参照して詳細に説明する。

図1は、請求項1～5に記載の本発明によるICカードサービス利用許可方法を実施する請求項6～10に記載のシステムの全体構成を示す。1はサービス提供者サーバ、2<sub>1</sub>、2<sub>2</sub>、...、2<sub>n</sub>は複数のサービス利用者サーバ1、2、...、n、3<sub>1</sub>、3<sub>2</sub>、...、3<sub>n</sub>はICカード、4はICカード読取装置4、5はICカード読取装置4とサービス提供者サーバ1とサービス利用者サーバ1、2、...、nを相互接続するネットワーク5である。

【0018】

サービス許可者サーバ1は、複数のサービス提供アプリケーションAP1、AP2、...、APnを複数のICカード1、2、...、nに提供しており、サービス提供アプリケーションを利用する複数のサービス利用者サーバ1、2、...、nへそれぞれサービス利用許可証の発行を行う。また、サービス提供アプリケーションにそれぞれ格納するサービス提供許可証を発行する。サービス利用者サーバ1、2、...、nは、任意のICカード内の任意のサービス提供アプリケーションと読取装置4及びネットワーク5を介して通信を行ってICカード保持者にサービスを提供する。以後、サービス提供アプリケーションはサービス提供APと略記する。

30

ICカードに格納されたサービス提供APは、サービス提供時にサービス利用許可証のチェックを行い、適切な利用者に適切な種類のサービス提供を行う。

ICカード保持者は、ICカード読取装置などを操作し、サービス利用者サーバ及びICカードからサービスを提供される。

40

【0019】

図2は、請求項3及び請求項8に記載の発明におけるICカード内のサービス提供APとサービス提供許可証の関係を示す。

ICカードには1つ以上のサービス提供APが格納されており、図では3つのサービス提供アプリケーションAP1、AP2、AP3が格納され、そのそれぞれのサービス提供AP1、AP2、AP3は、制御部の制御の下で通信手段を介してサービス許可者から受け取ったサービス提供許可証1、2、3を保持している。

【0020】

図3は、請求項1～4及び6～9に記載の方法及びシステムで使用するサービス利用許可証及びサービス提供許可証の構造を示す。

50

(a)は、請求項1～4及び6～9に記載の方法及びシステムにおいて、サービス提供者サーバがサービス利用者サーバに対し発行するサービス利用許可証を示し、このサービス利用許可証は、利用許可するサービス利用者サーバの公開鍵と、利用許可するサービス提供APのAIDと、サービスの種類（オペレーションの種類）等を含むサービス利用許可情報と、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。

(b)は、請求項4及び9に記載の方法及びシステムにおいて、サービス提供者サーバがサービス利用者サーバに対し発行するサービス利用許可証を示し、このサービス利用許可証は、利用許可するサービス利用者サーバの公開鍵と、利用許可するサービス提供APのAIDと、サービスの種類（オペレーションの種類）と、利用許可するデータの種類の等を含むサービス利用許可情報と、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。

10

(c)は、請求項8及び8に記載の方法及びシステムにおいて、サービス提供者サーバがICカードに格納されたサービス提供APに対し発行するサービス提供許可証を示し、このサービス提供許可証は、サービス提供APの公開鍵と、サービス提供APのAID等を含むデータと、そのダイジェストをサービス許可者サーバの秘密鍵で暗号化したデータ（署名）を含む。

#### 【0021】

図4は、請求項1、2に記載の本発明方法を実施するシステムの原理構成図を示す。

本システムは、ネットワーク5に接続されたサービス許可者サーバ1、サービス利用者サーバ2、ICカード3、ICカード読取装置4からなる。

20

サービス許可者サーバ1は、サービス利用許可証発行手段11を持ち、サービス許可者公開鍵ペアを保持する保持部12を持つ。

サービス利用者サーバ2は、制御部21と、署名生成手段22を持つ許可証管理部23と、サービス利用者公開鍵ペアとサービス利用許可証などを保持する許可証データ保持部24を持つ。

ICカード3は、通信手段31と、サービス提供アプリケーションAPIを持つ。

サービス提供APIは、制御部32と、署名対象データ生成手段33とサービス利用許可証検証手段34と署名検証手段35を持つ許可証管理部36と、サービス許可者公開鍵とサービス提供AP公開鍵ペアなどを保持する許可証データ保持部37と、サービス利用許可状態設定手段38と、サービス利用許可確認手段39と、サービス利用許可状態保持部40を持つ状態管理部41を持ち、更に、サービス実行手段42を持つ。

30

#### 【0022】

図5は、これらの手段を備える図4のシステムで実行される請求項1に記載のサービス利用許可方法の手順の一例を示すフローチャートである。

本システムでは、サービス許可者サーバ1のサービス利用許可証発行手段11が、保持部12のサービス許可者公開鍵ペアを用いて、図3aに示すサービス利用許可証1を予め発行している。

▲1▼このようなサービス利用許可証を持つサービス利用者サーバ2は、サービス提供APの利用時に、制御部21にて、ICカード読取装置5を通し、ICカード3に、チャレンジ（乱数）生成の要求を出す。

40

ICカード3では、通信手段31が、サービス提供APIの制御部32とサービス利用者サーバ2からの／への通信を仲介する。

▲2▼サービス提供APIの制御部32は、許可証管理部36内の署名対象データ生成手段33によって、乱数（チャレンジ）を生成・保存するとともに、サービス利用者サーバ2に送信する。

▲3▼サービス利用者サーバ2は、許可証管理部23内の署名生成手段22にて保持部24のサービス利用者秘密鍵で、乱数を暗号化して署名を作成し、その署名データと一緒にサービス利用許可証をICカード3に送信する。

▲4▼ICカード3内のサービス提供APIの制御部32は、許可証管理部36内の署名

50

検証手段 35 で、受信したサービス利用許可証に含まれるサービス利用者公開鍵を用いて、受信した署名データの検証を行う。また、▲5▼サービス利用許可証検証手段 34 で、許可証データ保持部 37 に保持しているサービス許可者公開鍵を用いて、受信したサービス利用許可証の検証を行う。

▲6▼これらの検証が成功したときは、状態管理部 41 内のサービス利用許可状態設定手段 38 で、サービス利用許可証の検証が成功したことと、サービス利用許可証に含まれる許可されたサービスの種類やサービス利用者公開鍵などのサービス利用許可情報をサービス利用許可状態保持部 40 に記録し、サービス利用者サーバ 2 に検証成功を返却する。

▲7▼サービス利用者サーバ 2 は、制御部 21 にて、サービス利用許可証に対応するサービスの実行を要求する。

▲8▼サービス提供 A P 1 の制御部 32 は、状態管理部 41 内のサービス利用許可状態確認手段 39 にてサービス利用許可状態保持部 40 を検索し、要求されたサービスがサービス利用許可証で許可済かどうかを確認し、許可済の場合は、▲9▼サービス実行手段 42 にサービスの実行を要求する。

従って、本システムによれば、サービス提供 A P は事前にサービス利用許可証の提示を受け、認証を行うことにより、正当なサービス利用者サーバのみにサービス提供 A P の利用を許可することができる。

尚、上記の例では、サービス利用者の署名データを先に検証し、次にサービス利用許可証を検証しているが、サービス利用許可証を先に検証し、サービス利用者の署名データをあとで検証してもよく、順番は問わない。また、署名対象データとして乱数を用いているが、他のデータを用いることができる。

【0028】

図 6 は請求項 2 に記載の方法の手順の一例を示すフローチャートである。

請求項 2 に記載のシステムでは、サービス提供 A P の利用時に、事前にサービス利用許可証の認証を行わないで、サービス提供 A P へのサービス実行要求時に、サービス要求許可証の認証を実行する。従って、本システムでは、▲1▼サービス利用者サーバ 2 は、サービス提供 A P 1 からチャレンジを受け取った後に、制御部 21 にてサービス実行要求を発生し、▲2▼署名生成手段 22 にて該チャレンジとサービス実行要求を含むデータもしくはそのダイジェスト情報にサービス利用者秘密鍵で署名を行い、この署名データをサービス利用許可証とともに IC カード 3 に送る。

▲3▼IC カード 3 内のサービス提供 A P 1 は、許可証管理部 23 にて、受信した署名データを受信したサービス利用許可証に含まれるサービス利用者公開鍵で検証するとともに、▲4▼受信したサービス利用許可証を、保持しているサービス許可者公開鍵で検証する。

▲5▼これらの検証が成功したとき、サービス提供 A P は、状態管理部 41 にて、サービス実行要求で要求されたサービスがサービス利用許可証に含まれるサービスの種類と一致するか確認し、▲6▼一致する場合に、サービス実行手段 42 にサービスの実行を要求する。

尚、本例では、サービス実行要求と一緒にサービス提供 A P からのチャレンジの署名を行っているが、このチャレンジの署名は省略してもよい。

【0024】

図 7 は、請求項 3 に記載の方法を実施する請求項 8 に記載のシステムの原理構成図を示す。請求項 3 に記載の方法は、サービス利用者サーバ 2 が通信相手であるサービス提供 A P を認証することができる。この目的のために、本システムは、図 4 に示す請求項 6 ～ 7 に記載のシステムの手段に加えて、サービス許可者サーバ 1 が、IC カードに格納されたサービス提供 A P 1 に、図 8 b に示すサービス提供許可証を発行するサービス提供許可証発行手段 13 を備え、IC カード 3 内のサービス提供 A P 1 がサービス許可者サーバ 1 により発行されたサービス提供許可証を許可証データ保持部 37 に保持するとともに、署名生成手段 38 を備え、サービス利用者サーバ 2 がサービス許可者公開鍵を許可証データ保持部 24 に保持するとともに、署名対象データ生成手段 25 と、サービス提供許可証検証手段 2

10

20

30

40

50

6と、署名検証手段27を備える。

【0025】

図8は請求項3に記載の方法におけるサービス提供許可証の認証手順を示す。

▲1▼サービス利用者サーバ2の制御部21が許可証管理部23内の署名対象データ生成手段25によってチャレンジ(乱数)を生成してICカード3に送る。

▲2▼ICカード3内のサービス提供APは、許可証管理部36内の署名生成手段38にて、受信した乱数をサービス提供APの秘密鍵で暗号化して署名を生成し、この署名データを許可証データ保持部37に保持しているサービス提供許可証とともにサービス利用者サーバ2に送る。

▲3▼サービス利用者サーバ2は、許可証管理部23内の署名検証手段27にて、受信したサービス提供許可証に含まれるサービス提供AP公開鍵を用いて、受信した署名データを検証するとともに、▲4▼サービス提供許可証検証手段26にて、保持しているサービス許可者公開鍵を用いて、受信したサービス提供許可証を検証することにより、サービス提供APの正当性を確認する。

尚、サービス提供APの署名データの検証とサービス提供許可証の検証の順番は問わない。また、署名対象データとして乱数を用いているが、他のデータを用いることもできる。

【0026】

【実施例】

実施例として、本発明を医療分野に適用した場合を示す。

サービス許可サーバは、医師会Xであり、ICカードアプリケーションである、電子カルテAP及び処方箋APを保持している。

サービス提供APは、これら電子カルテAP及び処方箋APである。

サービス利用者サーバは、医師会Xからこれらサービス提供APを利用する認可を受けている病院Aと病院B、薬局Cである。

病院Aは、処方箋APに関して、処方箋書き込みサービスに関するサービス利用許可証A1を保持している。

病院Bは、処方箋APを使用しない。

薬局Cは、処方箋APに関して、処方箋読み出しサービスに関するサービス利用許可証C1を保持している。

病院Aは、電子カルテAPに関して、電子カルテ書き込みサービス及び電子カルテ読み出しサービスを、対象データが病院Aの書き込みデータであるレコードに限定して許可している、サービス利用許可証A2を保持している。

病院Bは、電子カルテAPに関して、電子カルテ書き込みサービス及び電子カルテ読み出しサービスを、全てのデータを対象として許可している、サービス利用許可証B2を保持している。

薬局Cは、電子カルテAPに関して、電子カルテ読み出しサービスを、対象データが全ての病院の書き込みデータである場合において、全てのデータの、病院ID、診察日、診察医名の項目のみ許可している、サービス利用許可証C2を保持している。

これらのサービス利用許可証A1、C1、A2、B2は、全て、サービス許可サーバである医師会Xより発行されている。これらのサービス利用許可証A1、C1、A2、B2の例を図9の(a)～(e)に示す。

【0027】

また、処方箋APと電子カルテAPを格納したICカードを保有する利用者Dは、病院A、病院B、薬局Cをそれぞれ利用している。

利用者DのICカードに格納された処方箋APは、サービス提供許可証D1を保持しており、電子カルテAPは、サービス提供許可証D2を保持している。これらのサービス提供許可証D1及びD2の例を図9の(f)及び(g)に示す。

病院A、病院B、薬局Cにはそれぞれ、病院Aサーバ、病院Bサーバ、薬局Cサーバと通信を行うICカード読取装置が設置されている。

【0028】

10

20

30

40

50

利用者Dは病院Aで処方箋の書き込みサービスを受けることができる。図10はこの場合のシーケンスの一例を示す。利用者Dが、病院Aにて病院AのICカード読取装置にICカードを挿入すると、病院サーバAは、ICカード内の処方箋APと通信を行う。本例では、請求項3に記載の方法を用い、最初に、処方箋APは、病院Aのサービス利用許可証A1を確認し、病院Aサーバは、処方箋APのサービス提供許可証D1を確認する。この目的のために、本例では、最初に、

▲1▼病院Aサーバと処方箋APとの間でチャレンジ1及びチャレンジ2を交換する。

▲2▼病院Aサーバは処方箋APから受け取ったチャレンジ2を病院Aの秘密鍵で暗号化して署名を生成し、この署名データ2をサービス利用許可証A1とともに処方箋APに送り、処方箋APは送られてきた署名データ2を病院Aの公開鍵で検証するとともにサービス利用許可証A1を医師会サーバの公開鍵で検証して、病院Aのサービス利用許可証A1の正当性を確認する。

10

▲3▼正当性の確認後、処方箋APはサービス利用許可証A1に含まれるサービス利用許可情報を格納する。

▲4▼サービス利用許可情報の格納後、処方箋APは、病院Aサーバから受け取ったチャレンジ1を処方箋APの秘密鍵で暗号化して署名を生成し、この署名データ1をサービス提供許可証D1とともに病院Aサーバに送り、病院Aサーバは、送られてきた署名データ1をサービス提供許可証D1に含まれる処方箋APの公開鍵で検証するとともにサービス提供許可証D1を医師会サーバの公開鍵で検証して、処方箋APのサービス提供許可証D1の正当性を確認する。

20

その後、病院サーバAは、処方箋APに、処方箋情報の書き込みを行う。

【0029】

また、利用者Dは病院Aで電子カルテの書き込みサービスを受けることができる。図11はこの場合のシーケンスの一例を示す。利用者Dが、病院Aにて病院AのICカード読取装置にICカードを挿入すると、病院サーバAは、ICカード内の電子カルテAPと通信を行う。本例では、請求項2に記載の方法を用い、電子カルテAPは、病院Aのサービス利用許可証A2を確認した後、電子カルテ情報の書き込みを行う。本例では、最初に、

▲1▼病院Aサーバは、チャレンジ要求を電子カルテAPに送り、電子カルテAPから送られてくるチャレンジ2を受け取り、受け取ったチャレンジ2とサービス実行要求を病院Aの秘密鍵で暗号化して署名を生成し、この署名データをサービス利用許可証A2とともに電子カルテAPに送る。

30

▲2▼電子カルテAPは、受け取った署名データを病院Aの公開鍵で検証するとともに、サービス利用許可証A2を医師会サーバの公開鍵で検証して、病院Aのサービス利用許可証A2の正当性を確認する。

▲3▼サービス利用許可証A2の確認後、電子カルテAPは、サービス実行要求で要求されたサービスの種類（電子カルテの書き込み）がサービス利用許可証に含まれるサービスの種類と一致するか確認し、一致する場合に、サービス実行要求を電子カルテ実行手段及び病院Aサーバの制御部に送り、電子カルテの書き込みを行う。

【0030】

医師会Aは、請求項5に記載のように、サービス利用許可証の発行履歴をサーバ内に保存しており、発行履歴を参照して、病院A、病院B、薬局Cに課金を行う。

40

図12は、本実施例において、利用者Dが、病院A、病院B、薬局Cでそれぞれ電子カルテに記録されたデータの読み出しサービスを受ける場合の、読み出し可能なデータ範囲を示す。

【0031】

以上、本発明によるICカードサービス利用許可方法及びシステムの構成を説明したが、本発明システムを構成するサービス提供者サーバ、サービス利用者サーバ及びICカードの種々の手段はコンピュータにより実現され、本発明方法の処理手順はこれらのコンピュータにより実行され、本発明はこれらの処理手順を実行させるためのコンピュータプログラム及び該コンピュータプログラムを記録した記録媒体も本発明の範囲に含むものである

50

## 【0032】

## 【発明の効果】

以上に述べたように本発明によれば、次のような効果が得られる。

(1) サービス許可者が複数のサービス利用者に対してサービス利用許可証を発行し、ICカード内のサービス提供APがサービス利用許可証に基づいた実行制御を行うことによって、複数のサービス利用者が、自らはサービス提供APを開発することなく、1つのサービス提供APから提供されるサービスを利用することが可能となる。

(2) サービス利用者は、サービス提供APが持つサービス提供許可証を確認することによって、サービス提供APが、自らの保持するサービス利用許可証に対応する、正当なAPであることを確認することができる。

(3) サービス許可者は、複数のサービス利用者に、適切なサービスの提供を行い、サービス利用許可証を発行した代償として、サービス利用者に課金を行うことができる。

(4) 複数のサービス利用者が、1つのサービス提供APを使用するため、サービス提供APに対し、あるサービス利用者が登録したデータを、他のサービス利用者が参照するなど、複数サービス利用者間での、サービス提供APのサービスの共有が可能である。

(5) 同様に、複数サービス利用者間での、サービス提供APのデータの共有が可能である。

## 【図面の簡単な説明】

【図1】請求項1～5に記載の本発明のICカードサービス利用許可方法を実施するシステムの全体構成図である。

【図2】請求項3に記載の発明におけるICカード内のサービス提供APとサービス提供許可証の関係を示す図である。

【図3】請求項1～4に記載の方法で使用するサービス利用許可証及びサービス提供許可証の構造を示す図である。

【図4】請求項1、2に記載の方法を実施するシステムの原理構成図を示す。

【図5】請求項1に記載の方法の手順の一例を示すフローチャートである。

【図6】請求項2に記載の方法の手順の一例を示すフローチャートである。

【図7】請求項3に記載の方法を実施するシステムの原理構成図を示す。

【図8】請求項3に記載の方法の手順の一例を示すフローチャートである。

【図9】本発明の実施例における、サービス利用許可証A1、C1、A2、B2の例を示す図である。

【図10】本発明の実施例において、利用者Dが、病院Aで処方箋APの書き込みサービスを受けるサービス利用例のシーケンスを示す図である。

【図11】本発明の実施例において、利用者Dが、病院Aで電子カルテAPの書き込みサービスを受けるサービス利用例のシーケンスを示す図である。

【図12】本発明の実施例において、利用者Dが、病院A、病院B、薬局Cでそれぞれ電子カルテの読み出しサービスを受ける場合の、読み出し可能なデータ範囲を示す図である。

## 【符号の説明】

1 サービス許可者サーバ

2 サービス利用者サーバ

3 ICカード

4 ICカード読取装置

5 ネットワーク

AP1、...、APn サービス提供アプリケーション

11 サービス利用許可証発行手段

12 サービス許可者公開鍵ペア

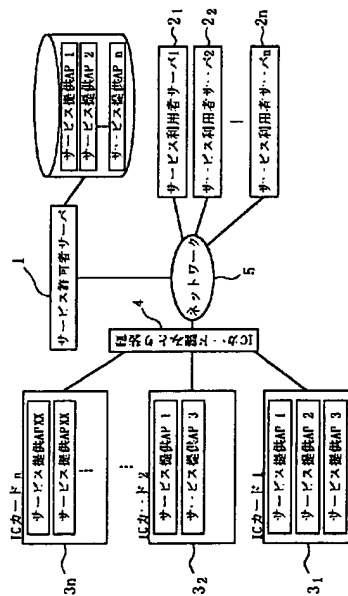
21 制御部

22 署名生成手段

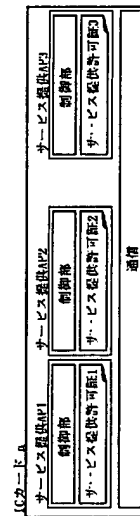
- 2 3 許可証管理部
- 2 4 許可証データ保持部
- 2 5 署名対象データ生成手段
- 2 6 サービス提供許可証検証手段
- 2 7 署名検証手段
- 3 1 通信手段
- 3 2 制御部
- 3 3 署名対象データ生成手段
- 3 4 サービス利用許可証検証手段
- 3 5 署名検証手段
- 3 6 許可証管理部
- 3 7 許可証データ保持部
- 3 8 サービス利用許可状態設定手段
- 3 9 サービス利用許可状態確認手段
- 4 0 サービス利用許可状態保持部
- 4 2 サービス実行手段

10

【図 1】

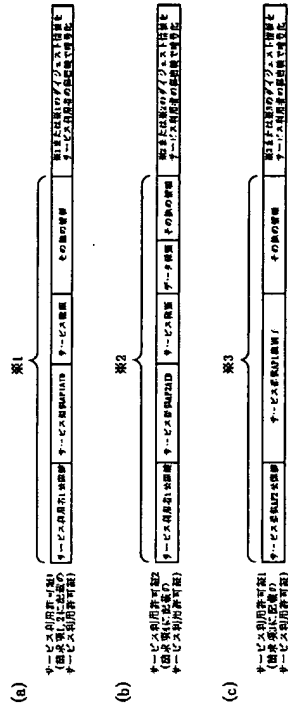


【図 2】

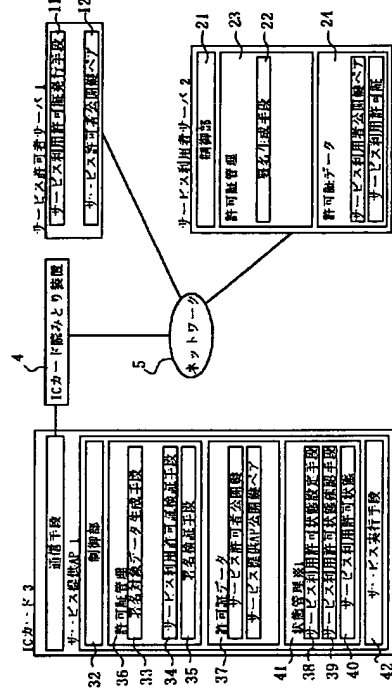




【図 3】

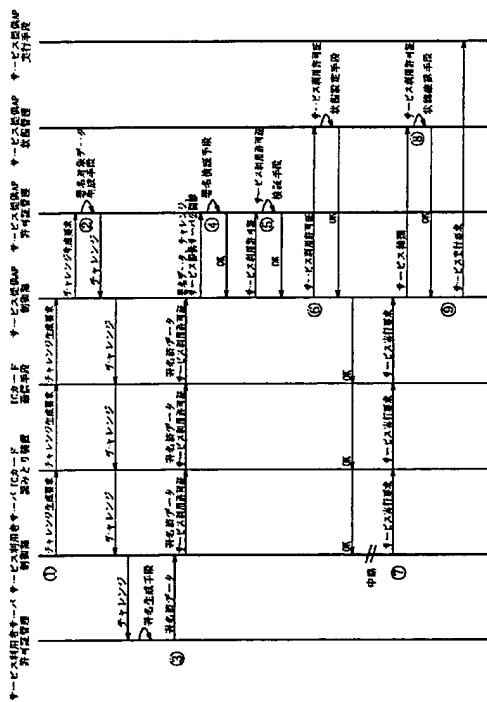


【図 4】

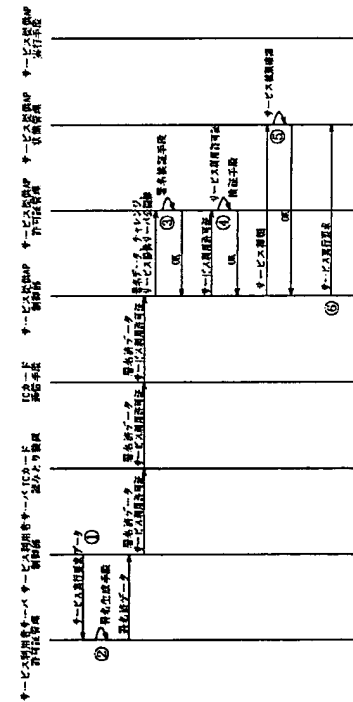


※1 請求項2においては不要

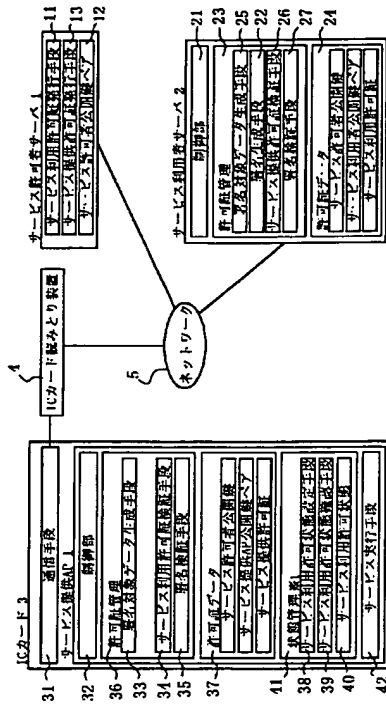
【図 5】



【図 6】

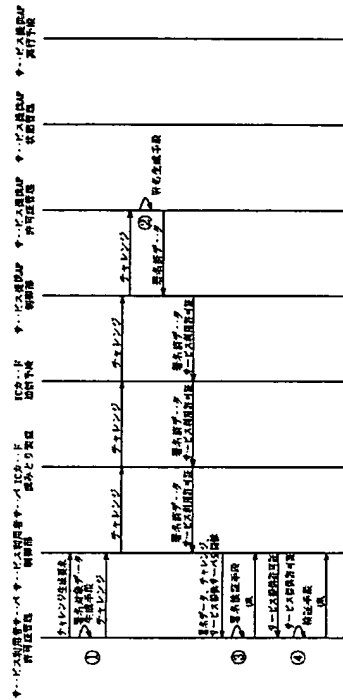


【 図 7 】

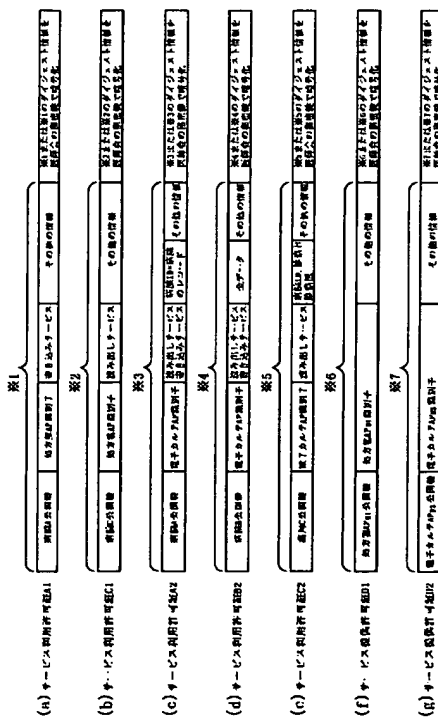


※1 請求項2においては不要

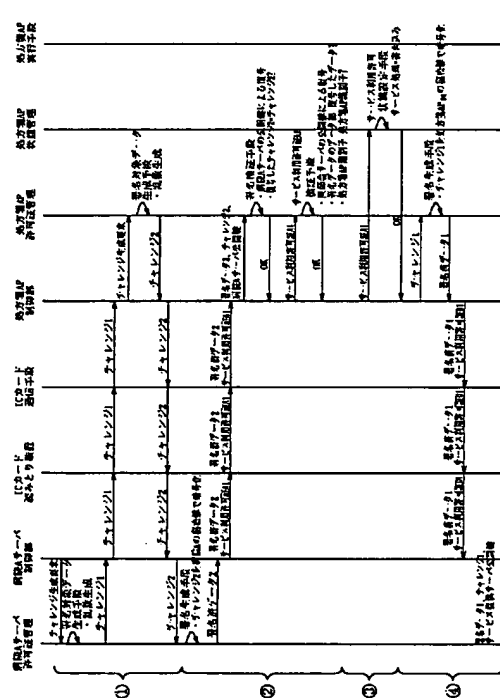
【 8 】



【 図 9 】



【 10 】



【 1 2 】



**アータ1**

- ・収録曲：収録曲
- ・収録日：昭和47年
- ・収録所：2004/4/7
- ・収録：収録、収録
- ・収録：収録
- ・収録：収録

**アータ2**

- ・収録曲：収録曲
- ・収録日：昭和47年
- ・収録所：2004/11/17/28
- ・収録：収録、収録
- ・収録：収録
- ・収録：収録

**アータ3**

- ・収録曲：収録曲
- ・収録日：昭和47年
- ・収録所：2004/12/7
- ・収録：収録
- ・収録：収録
- ・収録：収録

[illegible]

フロントページの続き

(51)Int. Cl.<sup>7</sup>

F I

テーマコード (参考)

H 0 4 L 9/00 6 7 3 E

(72)発明者 南 裕之

大阪府大阪市中央区馬場町 3 番 1 5 号 西日本電信電話株式会社内

Fターム(参考) 5B058 CA01 KA02 KA04 KA08 KA31 KA35 YA20

5B085 AE09 AE12 AE23 AE29 BE01 BE04 BG01 BG02 BG07

5J104 AA09 LA03 LA05 NA35

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**